Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
To: The Commission	)	

COMMENTS OF ZipDX

David Frankel
dfrankel@zipdx.com
17554 Via Sereno
Monte Sereno, CA 95030
Tel: 800-372-6535

Filed: June 27, 2017

Contents

EXECUTIVE SUMMARY

The robocall problem is massive and growing. Thankfully it seems to be moving from sideshow to center-stage at the Commission. There is the opportunity now to put sufficient intellect and firepower into mitigation efforts such that we might see a shrinking of robocall volume and associated complaints.

The NPRM and NOI are focused primarily on filtering solutions that depend entirely on a calling-line ID (CLID or caller-ID) that is provided by, and easily manipulated by, the robocaller. Robocallers will react to any obstacles that are placed in their path; such reaction must be anticipated when developing and prioritizing potential solutions.

We have studied the robocall problem extensively and have reviewed the NPRM solutions in detail. The data shows that these solutions will have no sustainable measurable effect on the robocall problem. Robocallers will quickly adapt, obviating any initial success.

Further, the NPRM solutions will invoke false positives that will cause legitimate calls to be blocked. Implementing these solutions is ill-advised. Because of the serious damage possible due to false positives, if blocking solutions are encouraged or even permitted, the calling party must be informed that their call has been blocked and why, and they must be offered a path to remove an improper block.

The NOI solicits input on other types of blocking solutions and makes mention of traceback and other efforts. Our analysis shows that the best way to block robocalls is to stop them at their source. Originating providers – that is, that part of the telecommunications industry that places calls onto the United States public switched telephone network as a service to end-users – are

ideally positioned to do this and we make explicit recommendations for how to engage them in doing so.

Traceback – the process of following a robocall from the call recipient backwards through the network to its source – is a critical element of successful mitigation efforts.

The FCC Enforcement Action just announced in June 2017[1] stiches this all together. This robocaller was placing a million calls per day or more using a different caller-ID for each time, making CLID-based blocking (whether in place or contemplated) ineffective. The calls were traced to the source and shut down. The $120 million fine puts this robocaller out of business and sends a strong message to his peers.

This process needs to be streamlined so that it can be efficiently applied on a much larger scale, commensurate with the scope of the problem.

We emphasize, as part of our analysis below, the distinction between originating, intermediate and terminating providers. The robocalling problem intersects the various segments of the telecommunications ecosystem in diverse ways. There are certain players whose practices aid and abet the robocallers, either by design or neglect. Those players should get special attention from the Commission.

Historically, discussion of the robocall problem has elicited comments that the problem is intractable. We conclude otherwise. The steps we propose are not technically complex and they are not expensive or time-consuming to implement, yet they focus on the fundamental characteristics of the largest robocalling campaigns. Still, they must be undertaken with

[1] Citation and Order, Prerecorded Message Violations and Wire Fraud, in the matter of Adrian Abramovich, Marketing Strategy Leaders, Inc. and Marketing Leaders, Inc, FCC DA-17-593, released June 22 2017. See also the associated Notice of Apparent Liability, FCC 17-80, of the same date.

determination, precision and cooperation by both regulators and industry stakeholders. That should not pose a barrier to deployment given their stated commitment to mitigating robocalls.

BACKGROUND ON SCALE AND THE NATURE OF ROBOCALLS

The illegal robocall problem is one of massive scale. It is the most complained about category in the federal government. The Commission estimates there are 2.4 BILLION robocalls placed per month.

Efforts to address this problem must respect its scale. Initiatives that will combat one million calls here or 10 million there will not make a dent in the problem. Arguing that such endeavors are "better than nothing" ring hollow; if the solutions have any cost at all, and if the predicted results are barely measurable, they really are not worth pursuing.

The United States public switched telephone network ("PSTN") is a complex network of networks based on a mix of sophisticated protocols. Individual network operators implement their own versions of the protocols and manage their interfaces with other networks using their own discretion. Thus, analysis of any initiative to eliminate robocalls that relies on any of those protocols requires study and understanding of real network traffic, rather than mere examination of published standards or recommendations.

In deciding which solutions to push forward, voice service providers must perform and document rigorous, critical, data-driven analysis of both the expected desired effects as well as the unintended side-effects. The scale problem works on both sides: With 2.4 billion robocalls per month, we need to think about stopping hundreds of millions per month in order to move the needle on the problem. (Assuming everything else is static, reducing the robocall problem by 20% requires that we stop 480 million – almost half a billion – such calls per month. And

reducing the problem by only 20% isn't going to be considered a success by consumers. At the same time, given that there are many (say, 10) billions of legitimate, desired telephone calls traversing the PSTN each month, if we interfere with the proper operation of just 0.1% of them, we have ruined 10 million conversations – made by hundreds of thousands of call originators and intended recipients every day.

Fortunately, since there is a constant flow of network traffic, we can observe the current environment and test, to some degree, the results of our planned actions. Operators keep, at least temporarily, logs of what is moving through their networks. A representative sample can reveal a treasure trove of information.

But also critical to the analysis is recognition that the robocalling environment is not static. Robocalling campaigns are driven by clever humans; they observe and react to their victims and their detractors. Sure as the water in a stream moves in a new direction when we drop a boulder in its path, robocallers will adapt to our deterrents. We must "think like a robocaller" to determine if and how they might circumvent our solutions, and thus to understand the sustainability of whatever mitigation efforts we undertake. A big investment to reduce robocalls by 20%, only to see them return to their original level 60 days later, is probably not worth the cost.

ASSESSMENT OF THE NPRM INITIATIVES

The NPRM proposes three specific initiatives, and codifies one other, to combat robocalls. The NPRM promotes blocking of calls which signal that they are from: invalid numbers, unallocated numbers, unassigned numbers, and numbers for which the subscriber has requested blocking.

All four of these initiatives suffer from common defects:

- They all rely, exclusively and fundamentally, on the calling line identity (CLID or Caller-ID) provided by the robocaller. This data element is easily manipulated by the robocaller such that he can readily and trivially defeat any of these mechanisms, should they be implemented.
- Even if the robocaller didn't bother to work around these mechanisms, examination of current robocalling patterns reveals that the number of robocalls falling into at least the first three categories is imperceptible on the scale of the current problem.
- Because of imprecision and outright error in the way that CLID is propagated to and through the PSTN, these schemes will suffer from false positives that will mysteriously block legitimate calls, leading to customer and service provider frustration. In some cases, calls from an entire business or a particular city-country combination could be erroneously blocked.

It is unfortunate that so much effort to date, and the NPRM, focus on the use of Caller-ID when these kinds of "filtering" solutions have long been acknowledged as having minimal potential impact. As far back as 2013, the FCC's Dr. Henning Schulzrinne explained to the North American Numbering Council regarding such approaches: "[T]hat while they might well so we hope provide some relief, they would primarily catch the dumb robo callers to be quite frank about it. … Unfortunately the fear is that as these type of techniques get deployed, namely that filters get deployed that the incentive to spoof will increase to bypass those filters."[2]

[2] Meeting of the North American Numbering Council, 18-September 2013, page 83. Transcript available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-326289A1.pdf.

Implementing the NRPM's solutions will simply result in those robocallers shifting to using other phone numbers. The number of robocalls won't be reduced.

The level of investment required to implement and maintain the proposed solutions would be better spent on more effective and sustainable deterrents.

I. Detailed Assessment of the NPRM Blocking Initiatives

A. Blocking at the Request of the Subscriber to the Originating Number

Section A of the NPRM proposes creation and maintenance of a "Do Not Originate" (DNO) list; carriers (presumably any carrier in the call path – originating, intermediate, or terminating[3]) could (and, implied by the NRPM, should) block such calls.

We certainly support the Commission giving carriers the authority to block calls which they reasonably believe to be in violation of established rules and likely to cause harm.

However, the specific DNO initiative is fraught with problems. As explained in the original "Robocall Strike Force Final Report"[4]:

- "We anticipate that success in blocking the high profile, official numbers will push the bad actors to randomly spoof numbers to continue their scams." Thus, DNO may have a TEMPORARY effect, but it will not result in a sustainable reduction in robocalls.

[3] Any given telephone call can involve multiple carriers: an originating carrier, zero or more intermediate carriers, and a terminating carrier (which can be the same as the originating carrier). Any final Order from the FCC should make clear, when referencing a "carrier" or "provider" exactly what role(s) in the call path are intended to be covered by a particular rule.

[4] 26-October-2016 Robocall Strike Force Report, available at https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf, page 33

Further concerns are explained in the most recent report of the Robocall Strike Force at section 4.3[5]:

- "USTelecom concludes that the DNO trials outlined in this report were effective due to the efforts being narrowly targeted towards the specific set of telephone numbers identified and confirmed as inbound-only. That is no guarantee that they will be similarly effective in the future, or that they could be successfully scaled without creating harmful unintended consequences. If DNO blocking procedures were more widely deployed beyond a narrow set of numbers (i.e., inbound-only telephone numbers), bad actors could easily and rapidly transition to randomized and/or legitimate telephone numbers in order to circumvent DNO blocks. In fact, the widespread deployment of a broader range of DNO numbers (e.g., unassigned telephone numbers) could have the perverse effect of quickly nullifying any protections, while also making robocallers more difficult to identify. This could also increase instances of both 'false positives' (i.e., blocking numbers that should not have been blocked) and 'false negatives' (i.e., fail to block numbers that should have been blocked)."
- "In the near term, any widely deployed efforts would likely face significant technical scalability issues, in addition to the policy risks (e.g. incentivizing more spoofing of legitimate numbers in order to get around DNO blocks) discussed above."

If that doesn't curb enthusiasm for DNO, perhaps this will. In its original report[6], the Robocall Strike Force reported on a test of DNO blocking of an IRS toll-free number, stating: "The IRS conveyed a 90% reduction in IRS scam call complaints in the last two months, with the

[5] 28-April-2017 Report of the Robocall Strike Force, available at https://ecfsapi.fcc.gov/file/10428085569795/Ex%20Parte-Strike-Force-Report-2017-04-28-FINAL.pdf, page 25
[6] Ibid, page 32

largest drop off coinciding with the DNO trial, from a high of 43,000 complaints in late August to only 3,700 complaints in mid-October."

The implication, of course, is that the DNO block was the cause of the complaint drop-off, and that this validates DNO as an effective robocall mitigation mechanism. But USTelecom's recent Ex Parte[7] explains "a series of arrests in India on October 5, 2016, effectively shut these fraudulent calls down at their source." Stopping the calls at the source, as the police in India were able to do, is the more likely cause for reduced calls related to this illegal scam.

The USTelecom DNO report presents evidence that demonstrates that the calls set to be blocked were, in fact, blocked – exactly what we would expect when the network engineers know what they are doing, which is often the case. What the report doesn't examine is what the robocallers did in response to these blocks.

Let's try a multiple-choice quiz asking the following hypothetical question: Suppose you are a robocaller and you have been spoofing a particular phone number belonging to a specific organization – the IRS or a law-enforcement agency – in an attempt to help legitimize your calls. Suddenly, you find that the telecommunications carriers are trapping calls that claim to originate from that particular number, and blocking them. At this point, you would:

A) Turn yourself into the authorities, admitting that you were illegally spoofing the number in an attempt to perpetrate an illegal scam, throwing yourself on the mercy of

[7] USTelecom Ex Parte, June 5, 2017, Do Not Originate (DNO) FCC Briefing, Kevin G. Rupy (available at https://ecfsapi.fcc.gov/file/1060525986960/USTelecom-DNO-Ex-Parte-2017-06-05-FINAL.pdf) page 9

the court and volunteering to divest yourself of any and all ill-gotten gains so that restitution can be made to those that you previously successfully defrauded.

B) Shut down your robocalling endeavor, and move on to some other form of malfeasance, such as running a Ferrari chop-shop or establishing an internet site for mail-order opioids.

C) Spend 30 seconds to alter the calling-line ID that you send, changing it, for example, from 800-CALL-FBI (225-5324) to 888-CALL-FBI or 800-TELL-FBI or 800-FBI-CALL or 800-J-EDGAR-H. (How many consumers have memorized the real FBI contact number?)

D) Spend 15 minutes programming your autodialer to send a (pseudo-) random number for each call.

All four of these responses would generate results consistent with the data presented in the USTelecom report. But the only LIKELY responses from robocallers are C and D, and now the DNO effort is completely defeated. Recipients of the resulting calls may dial back the number that they see on their Caller-ID display to ask "Why did you call me?" Instead of reaching the FBI, where they would get told, "Oh, that's a total scam, you need to ignore it" they will instead reach some other completely befuddled innocent party and now we'll have double the number of people annoyed. That will be the likely outcome of a diligent DNO effort.

B. Calls Originating from Unassigned Numbers

The NPRM proposes to allow blocking of "unassigned numbers" in three distinct categories. The NPRM states[8]: "[U]se of an unassigned number is a strong indication that the

[8] FCC 17-24, paragraph 16

calling party is spoofing the Caller ID to potentially defraud and harm a voice service subscriber."

The kinds of blocks are problematic – and, in the scale of the robocall problem, actually worthless – for the following reasons:

- Calls with calling-party ID's in the categories identified in the NPRM make up only a tiny fraction of all robocalls; these blocks will have no measurable impact on robocalling volume.
- Robocallers will easily work around this type of blocking, quickly rendering it ineffective.
- The unintended consequences of these blocks (false positives) are potentially quite troublesome and far outweigh any good that would result from successful robocall blocks.

For these reasons, carriers generally should not implement these blocks. However, if the CALLED party asks their provider (that is, the TERMINATING provider in the call path) to implement one or more of these blocks, the provider should not be prevented from doing so provided the customer is properly informed of the potential consequences and the blocked caller receives appropriate notice as noted below.

Similarly, if an ORIGINATING provider (that is, the first carrier in the call path) wants to screen the CLID provided by their customer and reject calls that have improper CLID, that should be encouraged.

The table below provides additional detail on each of the three blocking sub-categories identified in the NPRM.

1. Invalid Numbers	2. Unallocated Numbers	3. Unassigned Numbers
We analyzed approximately 3.5 million complaints in the FTC database (see our Appendix A). We used this as the best available proxy for actual robocall traffic. Each complaint includes a caller-ID; we calculated what fraction would be captured as "Invalid Numbers" and "Unallocated Numbers". (See table 1 in the Appendix).		
4.6% + 0.9% = 5.5%	2.1%	Uncertain, but likely < 2%
Initial impact if all three blocks were universally implemented across all carriers: < 10% Percentage of Robocalls Not Affected: 90%		
Technique(s) available to robocallers to work around the block: Exercise more care in choosing CLID; select CLID from a list of known good number ranges. (Applicable to all proposed filters)		
Level of effort / complexity for robocallers to work around the block:		
Trivial	Trivial	Trivial
Sustainable impact on robocalling from this type of blocking:		
None	None	None
Challenges in implementing this category of blocking:		
(a) A significant number of business PBX's are not properly configured and send only partial numbers (e.g., last 4 digits) as CLID. (b) Some calls transit antique networks that are not capable of transmitting CLID; and 0000000000 or similar phone numbers may appear for these cases. (c) International calls are often indistinguishable from NANPA calls, but will contain something other than ten digits, making them appear invalid, or will be 10 digits but with "invalid" NANPA NPA-NXX.	Some international numbers are ten digits but do not match valid NANPA patterns. For example, 479501XXX is a valid mobile number in Norway, but NXX 501 is unassigned in USA Area Code 479. 3255335XXX is a valid number in Belgium, but NXX 533 is unassigned in USA Area Code 325. In some cases numbers are not properly flagged as being E.164 (not a "national" number in our dialing plan). International calls from these geographies will be improperly blocked.	As noted in NPRM, there is no good database indicating which numbers fall into this category. Further, it would be extremely inefficient to have each carrier in the call path query a newly-created database for this info; that would slow call processing. Failure by providers to update the database as numbers change status, as well as caching, could result in newly activated numbers not being able to make calls due to improper blocking.

Potential impact / damage when calls are misidentified:		
An entire business (PBX) could be blocked from placing calls. Calls from countries or regions with country/city codes mis-matching NANPA NPA/NXXs could be blocked. (These apply also to categories 2 & 3 to the right.) Calls that transit older networks and thus lose proper CLID signaling could be blocked.	Newly-opened NPA-NXX codes could be blocked by providers that do not promptly update their blocking algorithms. See also Column 1.	Newly activated telephone numbers could be blocked by providers that cache in-service number lists. See also Column 1.

We have noted that there are significant possibilities of false positives in the blocking scenarios proposed. We know from experience with uncompleted calls to rural areas,[9] that when legitimate calls fail to complete, it can be terribly frustrating for both the calling and called parties.

We propose that, to the extent that the Commission allows (and certainly if it encourages) carriers to block calls, the Commission requires (1) that prior to implementing the block, the carrier analyze recent traffic to assess the likelihood of blocking legitimate traffic, and (2) that the block alerts the calling party to the nature of the block and how to resolve it.

With respect to traffic analysis PRIOR to blocking calls:

- The carrier should examine recent historical call detail records, or should generate records representative of those that WOULD be blocked if the proposed block were implemented. The call completion rate (what fraction of calls are actually answered)

[9] See, for example: https://www.fcc.gov/general/rural-call-completion-problems-long-distance-or-wireless-calling-rural-areas

and the distribution of call holding times (how long the called party stays connected to the caller) should be analyzed. Typical undesired robocalls have low call completion rates and very short hold times. If the analysis reveals that the characteristics of the calls proposing to be blocked do not fall within the range of values expected for known universe of robocalls, further investigation should be performed before implementing the block.

With respect to alerting the calling party, any carrier implementing a block should implement the following:

- An intercept that identifies the provider implementing the block, informs the caller why their call has been blocked, and gives them contact information allowing both US-based and international callers to reach a live operator 24 hours a day that can, in real time with appropriate explanation, suspend the block. (Virtually all providers are able to play recorded messages when they intercept calls.)
- Optionally, callers may be permitted to enter a short sequence of digits or speak a word or phrase that will demonstrate the call is legitimate and allowed to proceed.

Note that these intercepts are still problematic for those with limited English proficiency, for legitimately-placed automated calls, and for those using TDD, fax or other non-voice communications technologies.

The rules should provide an exception to the intercept requirement when the calling volume is so massive that the carrier is technically unable to play the intercept to all callers.

C. Conclusions Regarding the NPRM

Our analysis shows that the blocking initiatives in the NPRM are ill-advised. They rely on Calling Line ID which is inherently unreliable. The proposed solutions will have minimal impact because only a very small fraction of robocalls use affected CLIDs. Further, it is simple for robocallers to work around these blocks. Importantly, the blocks will prevent certain legitimate calls from completing, which will be quite problematic.

Resources that might have been devoted to implementing these blocks are better spent on other initiatives, which are discussed below.

INTRODUCTORY COMMENTS ON THE NOTICE OF INQUIRY

The Notice of Inquiry solicits input on other methods to mitigate robocalls. The most effective solution to the robocall problem is stopping them at the source. An analogy is in order.

If you find wasps around your home, threatening you, your children and your guests, you can try to swat them one at a time. You'll probably find that even if you kill 100 wasps this way, they keep coming.

Alternatively, you can try to find the wasps' nest. You can follow some wasps back to their nest. You don't have to successfully follow EVERY wasp; you just have to follow ONE all the way to the nest. If you can find the nest, you can wipe out the colony. Even if you just conclude they are coming from your neighbor's back yard, you can then enlist your neighbor to help eradicate them. Of course, she has to be willing to help.

This is going to prove a far more effective technique, whether the battle is against wasps or robocallers. And significantly, when an increasing number of robocallers are identified and

punished, other robocallers and would-be robocallers will take note, and these enforcement actions will serve as a real deterrent. Today, robocallers pursue their trade because all evidence indicates that they are extremely unlikely to be caught and punished.

Our PSTN is made up of many different service providers. Some are working diligently to combat robocalls; others are just along for the ride. But there are some service providers that are actually facilitating robocalling, and they need to be held accountable for the damage they are doing. Given the scope of this problem and the damage it is doing to the fundamental telephone service on which our society relies, aiding and abetting the robocallers is as unconscionable as the robocalling campaigns themselves.

There are numerous ways that service providers can be proactive in combatting robocalls that originate on their networks. The community of providers needs to be more engaged, more responsive, and more diligent in protecting the PSTN from illegal robocalls. The FCC needs to step up to its mandate from Congress to enforce the laws, not just with sporadic explicit enforcement actions, but with policies and guidance that will truly make a measurable impact on the problem.

The NOI seeks, in various forms, input on techniques that can be used to identify and block calls that are illegal or likely illegal "based on objective criteria." Before addressing the specific areas of input requested in the NOI, we offer the following.

As noted earlier, there are usually several providers involved in the completion of a single telephone call: originating, intermediate, and terminating providers. The NOI neglects to address this distinction, which is critically important because any given provider will be more or less effective in preventing robocalling depending on the role it plays in the call.

It is critically important to understand that the ORIGINATING PROVIDER is in the best position to mitigate robocalls. This is because the majority of robocalls come from a small number of perpetrators firing off thousands or hundreds of thousands of calls per hour. We draw this conclusion from anecdotal evidence as well as a study published by Pindrop Security at the 2016 Black Hat conference.[10] The paper's Abstract states: "Over several months, we recorded more than 100,000 calls and analyzed several million call records to validate our methodology. Our results show that only a few bad actors are responsible for the majority of the spam and scam calls…." In their Closing Remarks, they conclude: "We recorded about 100,000 calls from 44,000 source phone numbers. About one third of these calls were robocalls. Our results show that 51% of the robocalls recorded can be attributed to only 38 distinct telephony infrastructures…."

Thus, extrapolating from this data, if we could find those 38 "distinct telephony infrastructures" and block their calls (regardless of what CLID they used), we'd wipe out half the robocalls.

AT&T has recognized the power of blocking robocalls at the point of origination. In an April 2017 report on their blocking efforts[11], AT&T said: "It examines more than 1.5 billion calls each day for patterns that indicate robocallers. It then drills down on suspicious activity that may be illegal or forbidden. One example is multiple short-duration calls to numbers on the National Do Not Call list. … In recent weeks, the AT&T program has been averaging 12 million blocked

[10] The Pindrop paper is available at https://www.blackhat.com/docs/us-16/materials/us-16-Marzuoli-Call-Me-Gathering-Threat-Intelligence-On-Telephony-Scams-To-Detect-Fraud-wp.pdf
[11] The AT&T report is at http://about.att.com/story/more_than_one_billion_robocalls_blocked.html

calls per weekday. … The analytics-based blocking program works against those who use the AT&T network to *send* robocalls." (Emphasis in original)

Nomorobo, one of the better-publicized call blocking applications that operates at the TERMINATING end of the call, reports blocking about 250 million calls since its inception several years ago.[12] The still-nascent AT&T effort blocks that many calls in less than a month.

The April 2017 report from the Robocall Strike Force states: "In instances where calls are traced to their point of origin, this often enables investigating providers to work with the originating carrier to cease such calls initiated by its customer. Such efforts are also extremely valuable to law enforcement, since carriers' ability to trace calls through several networks can substantially assist law enforcement personnel in subsequent investigations."[13] As we explained earlier, that Strike Force report also explained how the IRS scam being run out of India was shut down at the source by Indian authorities, resulting in a dramatic reduction in complaints.

Thus it becomes clear that the most technically sound and least problematic approach to robocall mitigation is to stop the calls at their source. Below we will discuss in detail two key components that will make this effective:

- Proactive efforts by ORIGINATING PROVIDERS to limit the ability of robocallers to anonymously launch and sustain volume robocalling campaigns
- Information sharing and coordination among providers and enforcers to penalize violators

Our objectives need to be:

[12] A count of blocked calls is available at the Nomorobo home page, https://www.nomorobo.com/
[13] Ibid at page 21

1) Prevent the launch of new robocall campaigns whenever possible
2) Quickly trace new campaigns to their source and shut them down
3) Use enforcement as a deterrent to let others know that robocalling is now a game that will not end well for the perpetrator

To date, it seems that many providers and regulators, while "committed" to addressing the robocall problem, have a defeatist attitude. They believe that the problem is intractable, and that only some monumental, technically advanced and expensive solution will really solve the problem. They are convinced that it is a game of "whack-a-mole[14]" – that whatever we do to knock them down, the robocallers will reappear somewhere else. This won't be the case if the robocallers no longer enjoy total anonymity and more often than not get punished for their crimes or have their services shut down by the originating provider.

The on-going concern that many robocalls originate from outside the United States, and thus are outside our jurisdiction and so cannot be address, is also misguided. All foreign calls enter the US PSTN through a United States provider. That provider can act to mitigate the calls. And as is demonstrated by our IRS/India example, foreign authorities can be cooperative and even foreign perpetrators can be brought to justice.

II. Response to the Notice of Inquiry

A. Objective Standards to Identify Illegal Calls

The NOI requests, at 27, for input on identifying "presumptively illegal" calls. We promote two methods for identifying calls that need attention:

[14] "Whac-a-mole" is a registered trademark owned by Mattel, Inc.

- Calls to honeypot numbers, or similar systems such as voicemail platforms, where there is an audio recording that makes clear, along with the signaling information captured with the call, that it is illegal or otherwise abusive. For example, a caller that states "I'm with the IRS and you are about to be arrested" or "This is Microsoft and there is a problem with your Windows computer" or "I'm Cindy with Card Services. There is no problem with your account, but we can lower your interest rate" would all be indicative of illegal calls, since if nothing else they misrepresent the calling party and thus fail to properly identify themselves as required by the TCPA. A call back to the CLID would likely reveal that it does not reach the actual calling party, and assuming the called number is on the Do-Not-Call list, that would be another violation.
- Groups of calls originating from the same source that fail to meet certain call completion thresholds, experience particularly short hold times, or contain wildly disparate CLID values.

For each of the cases above, the calls would be identified after-the-fact; that is, we do not propose that this information be used to block the instant call. Rather, this information is used to identify the source of the calls and to block subsequent attempts.

At 30, the NOI asks about traceback efforts. Traceback should be used to find the source of the calls and to block them at the source. Verification of the legality of the calls can often be done by humans once the source is identified. There is no need for an "informed consumer" to make a decision about the veracity of blocking calls from a known illegal robocaller. Those calls should be blocked (that is, service to the perpetrator should be suspended) without any action by

a consumer – meaning no need to subscribe to some telephone company or third-party blocking service.

At 32, the NOI asks about Caller-ID Authentication Standards. It will be years before these technologies are sufficiently deployed such that robocallers cannot work around them. Neither the FCC nor legislators nor carriers nor consumer advocates should think for one millisecond that CLID Authentication will have any measurable impact on the robocalling problem in this decade. The FCC should not lead the general public to believe otherwise.

At 33, the NOI asks about Information Sharing. This is critically important for traceback efforts and should be required. Providers often cite fear of CPNI regulations for restricting what they share. As noted in the NOI, the FCC should remind providers that CPNI regulations carry a specific exemption permitting information sharing for the protection of the network and its customers. The FCC should make clear to providers that sharing information amongst their peers, or with third parties specifically engaged in efforts to stop abusive calling is permitted and encouraged. The FCC should prohibit providers from citing CPNI regulations to impede an otherwise legitimate investigation of a properly documented abusive calling incident.

Additionally, the FCC should require providers to maintain and distribute contact information, to include an email address and a telephone number, for an in-house resource to participate in industry abusive telephony mitigation efforts.

And the FCC should encourage the sharing among providers, regulators and enforcers of best practices and other information relevant to the mitigation of abusive telephone calls.

B. & C.: Safe Harbor for the Blocking of Calls Identified Using Objective Standards and Protections for Legitimate Callers

At 34 through 36, the NOI asks about a safe harbor to protect providers from accusations of improper blocking, and about protecting algorithms so that robocallers are not able to readily work around them.

At 37 and 38, the NOI asks about white-listing.

At 39 and 40, the NOI asks about legitimate callers that find their calls blocked – false positives.

We will address the last items (39/40) first. As noted in the NOI at 39, the terminating provider (that is, the provider serving the call recipient) may not be the one blocking the call. We noted earlier that the Commission must be very explicit about which providers in the call path are allowed to block calls, and what their responsibilities are when they do that. We proposed that if a provider chooses to implement a block, they must provide an intercept message that identifies the provider implementing the block and advises legitimate callers how to lift the block. A provider that cannot comply with this requirement should not block calls except in extenuating circumstances.

We noted in our discussion of Information Sharing that providers should have a point of contact for use by peers in addressing abusive calls. This should not be overly burdensome unless the provider is going out of their way to facilitate robocalling. NOI item 40 regarding contact information for legitimate callers is addressed in the paragraph immediately above.

Regarding the other items (34 through 38): The context of the NOI is that calls will be blocked by all manner of providers (originating, intermediate and terminating) using, it seems,

CLID as a primary trigger and maintaining blacklists and whitelists. This is doomed to fail (meaning that it will not scale to dent the robocall problem) and should be discarded.

- CLID is readily manipulated by the call originator. Robocallers will continue to find ways to do this for the foreseeable future, even as various mechanisms are put in place to restrict it.
- Blacklists are useless because robocallers will just use numbers not on the list.
- Whitelists are worse than useless because robocallers will learn of numbers on the whitelist and appropriate them for their own nefarious purposes. This not only defeats the whitelist but makes life even more miserable for the legitimate owners of whitelisted numbers.
- Maintaining blacklists and whitelists across providers is an administrative nightmare that will consume resources better spent on something productive.

Appendix A attached hereto presents data from the FTC's Do-Not-Call complaint database. Tables 5 and 7 show clearly that an increasing number of complaints are attributable to CLIDs that are used relatively infrequently, suggesting that robocallers are moving to randomizing their caller-ID or using "neighbor spoofing" (where they pick a pseudo-random CLID that makes it appear that the caller is a neighbor of the called party).

Given the futility of pursuing CLID-based solutions, the Commission needs to focus on addressing robocallers at their source, discussed next.

D. Requirements for Originating Providers and for Other Providers in the Call Path

As explained above, mitigation of abusive calls should be focused on the SOURCE of those calls. By far, there are a relatively small number of origination points for these calls, compared to hundreds of millions of termination points.

We propose two specific areas of focus for the Commission and the industry, which will provide the best return on investment in addressing the robocall scourge:

- Obligate Originating Providers (that is, those providing "termination service" which allows subscribers to make outgoing calls to the public network) to proactively protect the incoming boundaries of the network from abusive calls.
- Formalize the traceback efforts as piloted by USTelecom and require providers to participate in the traceback initiative.

We also propose outreach to all entities that enable robocalling, including making a clear distinction between telecommunications providers and their obligations, versus the requirements and liabilities placed on end-users of telecommunications services. This can serve as a safe harbor for these entities.

1. Obligating Originating Providers to Proactively Protect Against Robocalls

A robocalling campaign exhibits specific characteristics that differ from legitimate telephone traffic; these can be detected by the originating provider. Specifically:

- The robocaller makes outbound calls at a high rate, and this rate is sustained for a long period of time. For example, a robocaller might make 20 calls per second and do that for 10 hours throughout the day.

- Of the calls that are answered, a large fraction will be of a very short duration – either because the called party realizes it is an unwanted call and hangs up, or because it reaches voicemail and the robocaller hangs up.
- Many of the robocaller's attempts will go unanswered, either because he is calling a number that is not in use, or because the called party does not recognize the call as desirable and does not answer, and/or because the robocaller abandons the call after just a few rings.

Originating providers should be required to identify robocalling patterns and to proactively prevent illegal robocallers from accessing the PSTN. Where technically feasible, this includes both limiting the rate at which an end-user can initiate outbound calls and restricting the number of outbound calls that can be simultaneously active. It also means analyzing call records on at least a daily basis, if not more frequently, to identify any end-users with a pattern indicative of abusive calling.

To facilitate analysis of calling patterns, and to allow downstream providers to more readily identify suspicious calls, originating providers should be required to take steps to ensure that the signaling data in the calls they propagate are valid and correct. The Billing Telephone Number (distinct from the CLID) should properly reflect the end-user. If the CLID is not a number belonging to the end-user or authorized for the end-user's use, a Redirecting Number belonging to the end-user should be included. Where SIP signaling is employed, the comparable SIP headers should be used.

Originating providers should be required to immediately investigate suspicious calling behavior. For end-users generating legitimate traffic that triggers the thresholds for potential abusive calling, the provider should obtain and retain documentation that explains the nature

of the traffic and justifies any relaxation of rate and concurrent call limits. Similar requirements should apply for any relaxing of signaling rules. When relaxing constraints, the provider should perform proper vetting, including obtaining telephone, email and physical contact information for the end-user, and the provider should verify via human-to-human phone call that the end-user is legitimate.

Further requirements should be imposed on providers accepting calls from entities outside the United States, including those providing gateway services to international carriers. As a general rule, calls from outside the USA should not carry USA area codes in their CLID. Certainly there will be exceptions; roaming mobile subscribers and call centers engaged by US companies are two that come to mind. US providers serving overseas entities that lack justification for using USA area codes (with the +1 USA country code explicitly included or assumed) should be blocked from doing so. Otherwise, measured exceptions should be allowed as follows.

For the mobile case, traffic volumes should be relatively low. If there were one million Americans roaming outside the country (about one in 300), and each of them placed 5 calls per day back to the USA between 6 AM USA Eastern Time and 10 PM USA Pacific Time (a 19-hour window), there would be an average of 73 calls per second placed WORLD-WIDE from this group. US providers should use this kind of data to negotiate reasonable limits on the rates at which their overseas partners can place calls using a USA CLID. Mobile operators could better inform us regarding actual traffic history and the providers that would be expected to send these calls back to USA.

For the call center case, there would be specific CLID's which the centers are authorized to use by the USA number owners. USA providers should require their overseas partner to

obtain documentation from their end-user call-center customers exhibiting their authorization from the owners to use USA numbers.

2. Streamlining and Scaling Traceback Efforts

Once a robocalling campaign has launched, tracing it back to its source is key to shutting it down and deterring others from launching their own robocall campaigns. Squelching a new campaign quickly limits the damage like no other solution.

The Commission should designate an entity to serve as a Clearinghouse for traceback initiatives. USTelecom has already developed and prototyped this function as detailed in the April 2017 Strike Force Report. The Commission should quickly determine, with input from stakeholders, whether USTelecom should continue in this role, or if some other entity should assume this function. Factors for consideration should include but not be limited to:

- The scope for the Clearinghouse, including not just traceback but also intake of complaints, operation and/or collection of honeypot data, interface with enforcement authorities, development and distribution among providers of best practices, ongoing data analytics, outreach to others in the telephony ecosystem, publication of data to stakeholders (including providers, regulators, legislators, advocates and consumers).
- Level of technical expertise with respect to call signaling, network operations, database development and discovery, API development and deployment, system integration, network security, and automation.
- Funding and management. (We do not believe that the Clearinghouse function requires a significant staff, but it requires dedicated resources to maintain focus and agility. An operation with a staff of 6 could run on an annual budget of less than $2

million, which is less than one cent per active US telephone line subscription per year.) Even a passionate team of just one or two full-time equivalents, focused on the robocall problem, could have a huge impact if the industry support that has been pledged were actually delivered in the form of coordinated efforts along the lines outlined here.

In addition to monitoring, detecting and limiting robocalling activity, all Providers (originating, intermediate and terminating) should be required to participate in industry traceback efforts. Specifically, upon receipt of a bona fide request from designated entities (e.g., the Clearinghouse described above) a provider should be required to:

- Respond within 24 hours or less
- If acting as an intermediate provider, provide the identity of the upstream provider that delivered the call
- If acting as the originating provider, with the identity of the originating end-user and any on-file information detailing exceptions granted for traffic characteristics or call signaling compliance
- Cooperate under a non-disclosure agreement with the designated Clearinghouse entity and without requiring a subpoena or civil investigative demand or similar

A provider should be required, upon presentation of evidence that calls originating on their network are resulting in multiple complaints of abuse, to engage with their customer to determine the validity of the complaints and to promptly terminate service to that customer if the complaints are verified.

3. Further Engagement of Entities Providing Services to Robocallers

There are numerous ways that a high-volume robocaller can inject their calls into the PSTN:

- Connect their automated dialing system to a traditional TDM trunk (such as an ISDN-PRI) or a SIP trunk purchased from a carrier, a VoIP provider, or a reseller of such services. This is the technology that is generally used to connect office PBX systems. These services can readily scale to very high call volumes.
- Purchase service from a Voice Broadcaster. Voice Broadcasters are services that make automated calls on behalf of their customers, often using call lists and recorded messages provided by those customers.
- Use a SIM box, which allows calls to be placed over a mobile network under computer control, using individual wireless subscriptions (on a prepaid or postpaid basis, either legitimately or fraudulently obtained).
- Through various other means, including hacking into business PBXs or similar nefarious means.

These mechanisms can be used anywhere – within the US, or from another country with calls routed into the US via the internet or via PSTN connections. Indications are that the bulk of robocalling (both legal and illegal) comes via commercial agreements between the robocallers and their telecommunications providers.

There is an extensive ecosystem that serves robocallers. A Google search for "voice broadcasting" will reveal an extensive list of providers that will make calls on behalf of a robocaller. Similarly, a Google search for "voip dialer deck" lists SIP trunking providers that will accept short-duration traffic for termination to any USA PSTN destination.

Throughout these comments, we have highlighted the challenges of blocking calls at the point of termination, given that there are hundreds of millions of PSTN endpoints in the United States.

There are hundreds or perhaps even thousands of entities that can facilitate the origination of robocalls, but this universe is orders of magnitude smaller than the number of consumer endpoints. By focusing on this constrained universe – and stopping robocalls at their source – the problem becomes much more tractable. We will call this the Robocall Enablement Ecosystem; members of this ecosystem are "enablers".

There are several steps that should be taken along these lines:

- Just as the Robocall Strike Force has advocated for consumer education to raise awareness of the problem, the enablers need to be made aware of the Commission's interest the problem, the steps being taken to combat it, and the cooperation needed to address it. Enablers (including law firms and marketing organizations that advise robocallers) need to be educated as to prohibited behaviors, requirements required for legal robocalling, and penalties for violations. For relatively minimal expense, this information can be made available via website postings and explicit outreach to the Ecosystem. Such an undertaking could be a straightforward task for the Clearinghouse referenced earlier.
- Enablers should be working to ensure that the robocalls they facilitate are legal. The Commission can incent this cooperation by offering a bright line distinction. A robocall enabler can hold itself out as a telecommunications provider and comply with Commission rules and best practices. If the enabler chooses not to do that, then they subject themselves to treatment as an End User, meaning that they are the entity

> "placing the call" and are subject to those rules and the consequential penalties for violations. Publication of appropriate rules and best practices would define a safe harbor for these enablers, should they choose to avail themselves of it.

Focusing on the sources of robocalls will generate the best return on investment. These enablers are professionals and have a vested interest in the matter. Those that are enabling legal robocalls want to see those calls complete and their business to flourish Those that are unwitting parties to illegal robocalls are as interested as the rest of us in seeing them eliminated.

Very few telecom executives will tell you that they make a good living off of illegal robocalls. This traffic is generally unprofitable for the telecom provider and generates far more complaints than benefits.

During the preparation of these comments, the author happened to receive several voice-mail messages from an "IRS Scam" robocaller that indicating I'd shortly be arrested if I didn't call back to arrange settlement of my overdue IRS debts. The callback numbers that they left (four different numbers in four messages) belonged, I discovered, to two carriers: Peerless Network and Inteliquent. Those two carriers have some distinction because they appear disproportionately in the FTC complaint data. (See, for example, Table 3 in Appendix A; Peerless numbers appear in the top spots in the most recent reporting period; Inteliquent appears quite frequently in other periods.) This doesn't mean that the robocalls are placed via their networks, but rather that their numbers are being used by robocallers (typically through resellers) as the Caller-ID for their outbound calls, and (as in this IRS scam case) as callback numbers.

I reached out to officials at both carriers and explained what I'd found. (In all four cases, the humans answering my callbacks identified themselves as representatives of the IRS.) Both

carriers promptly shut down the numbers, foiling the scammer's scheme to have targets respond to their voicemails by calling back. When alerted to abuse of their numbers, Peerless has a practice of altering the CNAM entry for the number to say "FRAUD CALL" as a further way of alerting targets that the caller is perpetrating a scam.

The point is that these particular enablers are enthusiastic about stopping illegal robocalls. They just need to be informed, because in most cases, they don't even know that they are part of the problem. The industry needs to become more proactive and cooperative in banding together to mitigate illegal robocalls[15], and the Commission needs to use its authority and position to further that.

The Commission has obvious authority over telecommunications carriers, and has also promulgated regulations covering interconnected VoIP and non-interconnected VoIP providers. In prior enforcement actions[16], the Commission has exercised its authority over other enablers. Any enabler not cooperating with the Commission and the industry to stop illegal robocalls should be deemed an end-user and should be subject to all the stipulations of TCPA, Truth-In-Caller-ID, and similar laws and regulations, and liable for the applicable penalties when they are involved in prohibited calls.

CONCLUDING COMMENTS

The data presented here show that the actions proposed in the NPRM will not be effective and are in fact dangerous because they will block numerous legitimate calls.

[15] See our Appendix B, where we suggest a supplement to the commercial agreement that telecom wholesalers have with their customers. This supplement would mandate proactive steps to curb robocalling at the source.
[16] See, for example, In the Matter of Dialing Services LLC, May 8 2014, FCC 14-59, where the FCC held a Voice Broadcaster liable for calls placed on behalf of a client. Available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-59A1.pdf.

With respect to the NOI, we have emphasized the same strategy espoused by others – that stopping robocalls at their source provides the best return on investment.

Robocalling is a dynamic environment. It is a war with smart players on both sides adjusting their tactics dynamically. The Commission was effective in rallying an industry-backed Robocall Strike Force; the first iteration demonstrated a workable concept but the results have fallen short. This effort needs to be reconstituted in a form that can address the realities of the problem with appropriate passion, skills, commitment and resources.

Each day, thousands of consumers express their frustration with the Do-Not-Call list as they file complaints with the FCC and the FTC. It is telling that in the robocalling industry, what matters now is not the DNC list; we know that is ignored. What matters is the "I'll Sue You" list – robocallers access a list of known plaintiffs and avoid calling them.[17] This is the "real" do-not-call list that truly stops you from getting unwanted, illegal calls. This exemplifies the war we are waging.

It's time to step up the game and let the robocallers know they've met their match.

Respectfully submitted,

DATED: 27 June 2017

/s/ David Frankel

dfrankel@zipdx.com
Tel: 800-372-6535

[17] See, for example, http://www.dnc.com/sites/default/files/Litigator%20Scrub%20Overview_0.pdf – "Scrub your List for Known Litigators Today" and http://www.donotcallprotection.com/ -- "Is a Previous Litigator Scrub important today?" and http://www.dncsolution.com/ -- "Litigator List helps you prevent TCPA and debt collection-related lawsuits by identifying plaintiffs and attorneys who have previously been involved in multiple lawsuits"

APPENDIX A

FTC COMPLAINT DATABASE ANALYSIS

This appendix contains various figures resulting from an analysis of the FTC Do-Not-Call complaint database. The FTC receives far more complaints about unwanted calls than does the FCC. How consumers decide where to direct their comments is unclear, but it seems that the FTC intake mechanisms are more widely promoted.

The FTC offers an extraction of its database for public download on a two-week cycle. The data made available is simply the date and time of the complaint and the calling telephone number, both as input by the complainant.[18]

We examined 30 weeks of FTC data – the fifteen files covering the period 16-October-2016 to 13-May-2017. In addition to parsing the reported telephone numbers to determine their validity, we also cross-referenced the (potentially valid, non-toll-free) numbers to industry databases to determine the Local Operating Company to which each number is assigned, and we attempted to find a calling-name entry for the numbers reported more than once.

With this set of data loaded in a relational database, we were then able to perform a variety of queries to glean insights potentially relevant to the subject NPRM/NOI.

While the database contains information only from complaints filed by the public, we believe it is representative, to a first-order level of accuracy, of robocall traffic in general. It is of course imperfect – it will contain typographical errors and perhaps purposefully fabricated entries. It has not been vetted for which calls are in fact "illegal" versus those that are allowed by regulation. Nonetheless, it is informative and we don't believe that the imperfections in the data (or small errors that we may have made in our analysis) undermine the conclusions we draw from it.

We have posted that portion of our dataset containing 10-digit calling numbers at [http-to be determined] so that others may readily download it and preform their own analyses. The posted data excludes the calling-name information, since that was obtained under a restrictive license.

In the tables below, we make reference to numbers and complaints:

- A complaint is a report of a robocall at a particular date and time and includes a calling number field. There were about 3.5 million complaints during the study period.
- A number is a value (typically a telephone number, but sometimes it is a blank string or it is an invalid phone number like 45678) that has been reported as the calling number associated with a complaint. There are about 653,000 UNIQUE 10-digit number values in

[18] Recent FTC complaint data is available for download at https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/frequently-requested-records#donotcall. It would be even better if the FTC named the files consistently; today they sometimes use a name like donotcall_violations_sept18_oct1_2016.csv, or february_19_2017-march_4_2017.csv or dontocall_violations_dec11-24_2016.csv making it challenging to find older data.

the database; some appear only once, while in other cases, the same number value is reported in thousands of complaints. Our focus here is 10-digit numbers.

Note that we have attempted to combine LECs across state boundaries based on LEC name.

Number Type	Examples	Unique Numbers	Complaints	% of all Complaints
Not 10 Digits	Blank, 54658, 50936785606		164,832	4.6%
10 Digits but Invalid in NANP	0000000000, 8170247862	10,355	33,984	0.9%
Unallocated NPA-NXX	2029460397, 2108686646	34,279	74,380	2.1%
Toll-Free 8YY	8556534481, 8006427676	30,822	248,810	6.9%
Other Geographic 10 Digits	4044559111, 8042900000	577,616	3,063,468	85.5%
TOTAL		**653,072**	**3,585,474**	**100.0%**

Table 1: Calling Numbers Throughout Study Period

Rank		Entire Study Period			
		Number	LEC	Calling Name	Complaints
1		8556534481	TollFree	TOLL FREE CALL	4488
2		8887271127	TOLLFREE	TOLL FREE CALL	3551
3		2012851836	CTCComm	GREEN	2873
4		8002551412	TollFree	TOLL FREE CALL	2804
5		3059855505	Bandwidth	UNKNOWN NAME	2748
6		8042981773	LocalAccessLLC	LOCAL	2104
7		5162310987	LocalAccessLLC	ASSIST	1887
8		9167588621	Onvoy	CUST SERVICE	1871
9		5303929040	Onvoy	GREEN	1854
10		7182589053	Verizon	NEW YORK	1839

Table 2: Most Frequently Reported Numbers (Entire Study Period)

Rank	Most Recent Period			
	Number	LEC	Calling Name	Complaints
1	5134577603	Peerless	CUSTOMER SERVIC	952
2	5403289788	Peerless	CUST SERVICE	857
3	4432589328	Peerless	VOIP CALL	849
4	5202100610	Peerless	SUPPORT LINE	829
5	8172030453	Peerless	CUST SERVICE	799
6	4192208338	Peerless	SUPPORT LINE	741
7	2312377277	Peerless	CUST SERVICE	736
8	4342053966	Peerless	CUST SERVICE	723
9	3475375793	Peerless	UNKNOWN NAME	723
10	7602067422	Peerless	SUPPORT LINE	660

Table 3: Most Frequently Reported Numbers (Most Recent 2 Weeks)

# of 2-Week Periods	Numbers	Complaints	% of All Numbers	% of All Complaints
1	531,833	759,353	81.4%	22.2%
2	57,864	437,567	8.9%	12.8%
3	23,632	371,673	3.6%	10.9%
4	12,819	314,327	2.0%	9.2%
5	8,315	254,995	1.3%	7.5%
6	5,436	199,875	0.8%	5.8%
7	3,864	175,043	0.6%	5.1%
8	2,653	182,703	0.4%	5.3%
9	1,946	162,439	0.3%	4.7%
10	1,282	111,914	0.2%	3.3%
11	892	78,841	0.1%	2.3%
12	732	81,551	0.1%	2.4%
13	594	64,767	0.1%	1.9%
14	506	63,189	0.1%	1.8%
All 15	704	162,405	0.1%	4.7%
More Than 1	653,072	3,420,642	100.0%	100.0%

Table 4: Tally of Numbers by Number of Reporting Periods In Which They Appear

2-Week Period	Complaints			Numbers		
	Total	w/ 10D Number	% 10D	Distinct in Period	New from Last	% New
17:0430-0513	292,275	278,431	95%	100,767	70,168	70%
17:0416-0429	335,216	319,196	95%	96,736	65,079	67%
17:0402-0415	305,123	291,048	95%	85,880	55,588	65%
17:0319-0401	291,796	277,496	95%	85,849	55,562	65%
17:0305-0318	265,192	252,551	95%	75,395	48,755	65%
17:0219-0304	267,496	254,739	95%	70,023	44,110	63%
17:0205-0218	304,090	289,754	95%	70,894	45,748	65%
17:0122-0204	321,265	305,784	95%	67,372	44,384	66%
17:0108-0121	234,511	223,933	95%	54,689	35,911	66%
16:1225-0107	154,393	147,955	96%	40,022	24,983	62%
16:1211-1224	157,748	151,116	96%	41,714	26,264	63%
16:1127-1210	173,203	165,992	96%	43,748	28,687	66%
16:1113-1126	145,010	138,741	96%	39,625	25,864	65%
16:1030-1112	162,314	155,550	96%	45,521	33,712	74%
16:1016-1029	175,842	168,356	96%	48,257		
TOTAL	3,585,474	3,420,642	95%	653,072		

Table 5: Summary of Complaints and Numbers by 2-Week Period

2-Week Period	>1K Complaints/#		100-999 Complaints/#		10-99 Complaints/#		2-9 Complaints/#	
	#s	Complaints	#s	Complaints	#s	Complaints	#s	Complaints
17:0430-0513	0	-	219	42,199	3,962	94,353	18,943	64,236
17:0416-0429	1	1,047	318	69,403	4,504	108,280	20,118	68,671
17:0402-0415	1	1,158	255	47,586	4,376	114,849	19,122	65,329
17:0319-0401	2	2,223	163	29,619	4,699	116,297	20,090	68,462
17:0305-0318	0	-	179	30,766	4,366	107,961	17,635	60,609
17:0219-0304	0	-	264	48,461	3,921	100,049	16,395	56,786
17:0205-0218	2	2,762	366	65,667	4,184	114,107	16,684	57,560
17:0122-0204	2	2,521	446	97,592	3,989	102,290	16,098	56,544
17:0108-0121	1	1,053	343	57,801	3,022	79,851	13,619	47,524
16:1225-0107	1	1,180	162	28,816	2,137	54,832	10,186	35,591
16:1211-1224	0	-	120	21,166	2,397	62,688	11,140	39,205
16:1127-1210	0	-	147	26,120	2,708	69,897	11,646	40,728
16:1113-1126	0	-	90	16,155	2,306	59,120	10,534	36,771
16:1030-1112	0	-	125	21,198	2,439	61,469	12,055	41,981
16:1016-1029	2	2,190	143	24,078	2,711	65,592	12,484	43,579
All Periods	127	171,482	4,795	1,096,046	43,727	1,202,354	132,440	478,787

Table 6: Numbers Appearing in Multiple Complaints in a 2-Week Period

2-Week Period	#'s w/ 1 Complaint in Period		
	#s	Complaints	% of Complaints
17:0430-0513	77,643	77,643	28%
17:0416-0429	71,795	71,795	22%
17:0402-0415	62,126	62,126	21%
17:0319-0401	60,895	60,895	22%
17:0305-0318	53,215	53,215	21%
17:0219-0304	49,443	49,443	19%
17:0205-0218	49,658	49,658	17%
17:0122-0204	46,837	46,837	15%
17:0108-0121	37,704	37,704	17%
16:1225-0107	27,536	27,536	19%
16:1211-1224	28,057	28,057	19%
16:1127-1210	29,247	29,247	18%
16:1113-1126	26,695	26,695	19%
16:1030-1112	30,902	30,902	20%
16:1016-1029	32,917	32,917	20%
All Periods	472,018	472,018	14%

Table 7: Numbers Appearing In Only A Single Complaint in a 2-Week Period

Availability of this data for further analysis: To promote a team effort in addressing the robocall problem, we have made our dataset available for download via the web, should anyone be interested in using it in ways perhaps more creative than what we have already presented. Commenters are also welcome to use it to validate the data we have presented in the tables above.

The .csv file contains 653,072 rows plus a first row containing column headings. The first column is the 10-digit telephone number. The next 15 columns represent the number of complaints reported for that telephone number in a given FTC two-week complaint-data period, with column two containing complaints in the most recent period (starting 30-April-2017), and the 16th column showing the oldest period (starting 16-October-2016). The next column is the name of the LEC (per the LNP database) that owns the telephone number (as of the time of our analysis during the month of June); in most cases we have removed state distinctions for common LECs. Next is the total number of complaints for the number during the study period (sum of columns two through sixteen). Next is a flag indicating whether the number has been ported. The last column indicates in how many reporting periods the number appears (so it ranges from 1, indicating that the telephone number only appeared in a single two-week report, to 15, indicating it appeared in all of the reports).

Our file does not include the CNAM data, because it was obtained with licensing restrictions that leave us reluctant to publish this data.

The file (approximately 42 megabytes) is available at
https://drive.google.com/open?id=0BwMMmUvecqQ0Xy1yc1pqSXZmX2c

APPENDIX B

SAMPLE SUPPLMENT TO PROVIDER TERMS & CONDITIONS

This text supplements the commercial agreement between a Telecommunications Provider (TP) and its Customer. TP has agreed to provide telecommunications services to Customer for a fee or other consideration (including, for example, mutual exchange of traffic).

TP is committed to doing whatever it reasonably can to prevent calls that are illegal or otherwise violate applicable regulations. TP also is also committed to preventing abusive calls, which it defines as collections of calls, either from the same source or matching a particular pattern, which result in a disproportionate number of complaints from call recipients.

To meet these commitments, TP places the following requirements on Customer; Customer, by using the services of TP, agrees as follows:

Customer may act as an End User or as a Reseller of TP services, or both.

1. As an End User:

   a. Customer is fully responsible and liable for compliance with applicable laws and regulations of the United States, and those of any other country through which calls placed via TP services may pass or terminate. Customer is prohibited from placing calls in violation of these laws and regulations and agrees not to do so.
   b. Customer place no more than 10 calls in any 60-second period, except as provided below.
   c. Customer will have no more than 10 concurrent calls, except as provided below.
   d. For every call placed, Customer will signal a valid and correct calling party identity (CLID). Customer will provide TP, in advance, with all CLID numbers (whether owned or authorized) that it intends to use, except as provided below. If the CLID is a number other than a number for which Customer is the owner of record, Customer will have written authorization from the owner of record permitting Customer to use the number. Said written authorization will be shared promptly with TP upon request from TP.
   e. All calls placed by Customer via an automated telephone dialing system (as defined by the FCC) will contain CLID that meets the following criteria when called back: (a) Whether answered by a human or a machine, immediately provides full and correct identification of the party authorizing the original call; (b) offers, between 8 AM and 5 PM in the timezone of the originally-called party, direct access to a human that can reliably and accurately answer questions about the original call; (c) provides an expeditious way for an originally-called party to add their number to a Customer-maintained Do-Not-Call list (notwithstanding any obligation Customer may already have to honor an existing governmental Do-Not-Call list) and such Do-Not-Call instructions will become effective immediately to prevent any further automated calls from Customer to that originally-called party.
   f. To secure an exception to the call pacing, simultaneous calling and/or call signaling requirements listed above, End User will complete and submit an application detailing

the nature of their calling and the exception(s) required. Once approved, End User will update the application should there be any change to the representations made in the application.

2. If a Reseller:

a. Customer will require its customer (whether another reseller in turn, or an end-user) to agree to terms and conditions substantially identical to those contained herein.
b. Customer will impose on its End Users the rate limits and signaling requirements contained herein (above), preferably by monitoring them in real-time. If Customer is unable to monitor in real-time, customer will perform audits, at least every 24 hours, of End User traffic. Calls not in compliance with the requirements will be blocked.
c. For all calls placed by an End User, Customer will insert or screen for a working Billing Telephone Number linked to that End User and meeting the requirements of (1)(e) above.
d. If Customer permits an End User to apply for exceptions to the End User rules listed above, Customer will thoroughly vet the application before granting any exception, including obtaining physical address information for End User and verifying email and telephone contact information.
e. Customer will endeavor to prevent a single end-user from opening multiple accounts or using other techniques to circumvent the intent of the End User constraints listed above.
f. Customer will accept from TP or a bona fide industry traceback clearinghouse or a Regulator a list of one or more calls reasonably believed to be illegal or abusive, each call being identified by the date and time it was placed and the destination telephone number, Customer agrees to share, within 24 hours of the request, all signaling details associated with the call(s) as well as the identification of the Customer's customer placing each call and, if the Customer's customer is an End User operating under an exception, the details of that exception.
g. Customer will have a system for routinely auditing traffic from its customers and end-users to identify suspicious calling and will promptly investigate and resolve any anomalies.

Customer further agrees:

3. If more than 20% of completed calls are equal to or less than 6 seconds in length (a "Short Duration Call"), or if more than 35% of total call attempts do not complete during any given month per trunk group during any billing cycle (the "Incomplete Call Threshold"), then TP may bill a surcharge equal to 120 seconds (2 minutes) of conversation time for (i) each Short Duration Call or (ii) incomplete call above the Incomplete Call Threshold.

4. TP may in its sole discretion temporarily block duplicate or repeated numbers dialed in succession or abnormally short duration calls where Provider considers the number of attempts to be potentially harmful to the network. Provider shall have no liability for damages of any type for actions taken to protect the integrity of its network.